PERANCANGAN APLIKASI KRIPTOGRAPHY – ADVANCED ENCRYPTION STANDARD

TUGAS AKHIR

Disusun Oleh :

DEDY BUDIAWAN
NPM. 0534010171

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
S U R A B A Y A

2010

KATA PENGANTAR

Syukur *Alhamdulillaahi rabbil 'alamin* terucap ke hadirat Allah SWT atas segala limpahan Kekuatan-Nya sehingga dengan segala keterbatasan waktu, tenaga, pikiran dan keberuntungan yang dimiliki penyusun, akhirnya penyusun dapat menyelesaikan Skripsi yang berjudul **"Perancangan Aplikasi Kriptography – Advanced Encryption Standard"** tepat waktu.

Skripsi dengan beban 4 SKS ini disusun guna diajukan sebagai salah satu syarat untuk menyelesaikan program Strata Satu (S1) pada jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN "VETERAN" Jawa Timur.

Melalui Skripsi ini penyusun merasa mendapatkan kesempatan emas untuk memperdalam ilmu pengetahuan yang diperoleh selama di bangku perkuliahan. Namun, penyusun menyadari bahwa Skripsi ini masih jauh dari sempurna. Oleh karena itu penyusun sangat mengharapkan saran dan kritik dari para pembaca untuk pengembangan aplikasi lebih lanjut.

Surabaya, Desember 2010

(Penyusun)

UCAPAN TERIMA KASIH

Selama pelaksanaan Tugas Akhir dan dalam penyelesaian penulisan laporan Tugas Akhir ini, penulis mendapatkan banyak bantuan dan bimbingan dari berbagai pihak. Karena itu, penulis ingin mengucapkan terima kasih kepada :

1. Bapak Ir. Teguh Sudarto, MM selaku Rektor Universitas Pembangunan Nasional ”Veteran” Jawa Timur.
2. Bapak Ir. Sutiyono. MT, selaku dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional ”Veteran” Jawa Timur.
3. Bapak Basuki Rahmat. SSi, MT, selaku Kepala Jurusan Teknik Informatika Universitas Pembangunan Nasional ”Veteran” Jawa Timur.
4. Bapak Prof. Dr. Ir H. Akhmad Fauzi, MMT selaku dosen wali.
5. Bapak Nurcahyo Wibowo, S.Kom, M.Kom, Bapak Achmad Junaidi, S.Kom, M.Kom, Bapak Ir. Kemal Wijaya, MT, Bapak Chrystia Aji Putra, S.Kom, Bapak Wahyu S.J Saputra S.Kom selaku dosen pembimbing, penguji sidang tugas akhir dan lisan yang telah memberikan banyak kritik dan saran serta memberikan wawasan yang lebih luas.
6. Seluruh dosen teknik informatika yang telah memberikan ilmu, wawasan, tenaga dan waktunya dalam mengembangkan wawasan serta ilmu berkaitan dengan informasi dan teknologi.
7. Kedua Orang Tua, Adik (Luky) dan Keluarga Besar yang ada di Nganjuk tercinta atas motivasi dan doanya sehingga semua yang dikerjakan dapat berjalan lancar.
8. Yunita Dewi (Dyta) yang selalu menyayangiku.

9. Buat sahabat dan teman-temanku, terima kasih telah menjadi sahabat dan teman yang baik buat aku. Tulus, Sari, Ricky Hedi Aprianto, Aripin, M. Bagus Kurniawan, Ferry Syaifullah Arifin, Ahmad Naiim, Dodik Irmawan, Vidi, Apza rhee, Yoehar Tubagus Syaifullah, Ibrahim tauhid, Dido, Eka Wijaya Kurniawan, Rizal Hakim, Bagus Burhanun Na'im, Khoirul Huda, Ibnoe Qoyim, Yogie, Muslim dan teman-teman semua yang belum disebutkan, terima kasih banyak atas do'a dan nasehatnya. Sukses selalu buat semua.
10. Dan semua pihak yang tidak dapat disebutkan satu persatu.

Penulis menyadari sepenuhnya masih terdapat banyak kekurangan dalam penyelesaian penulisan laporan Tugas Akhir ini. Segala kritik saran yang bersifat membangun sangat diharapkan dari semua pihak, guna perbaikan dan pengembangan dimasa yang akan datang. Akhirnya besar harapan penulis agar laporan ini dapat diterima dan berguna bagi semua pihak. Amin…

Surabaya, Desember 2010

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Seiring dengan perkembangan zaman, kebutuhan manusia meningkat. Termasuk kebutuhan akan informasi. Oleh sebab itu, pengiriman dan penyimpanan data melalui media elektronik memerlukan suatu proses yang mampu menjamin keamanan dan keutuhan dari data tersebut. Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian. Enkripsi dilakukan ketika data akan dikirim. Proses ini akan mengubah suatu data asal menjadi data rahasia yang tidak dapat dibaca. Sementara itu, proses dekripsi dilakukan oleh penerima data yang dikirim tersebut. Data rahasia yang diterima akan diubah kembali menjadi data asal. Dengan cara penyandian tersebut, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan, melainkan hanya oleh penerima yang memiliki kunci dekripsi. Didorong oleh kegunaan yang penting tersebut, teknik (algoritma) penyandian telah berkembang sejak zaman dahulu kala. Mulai dari era sebelum masehi, hingga sekarang algoritma penyandian ini selalu berkembang. Pertimbangan bahwa sebuah standard algoritma yang baru sangatlah diperlukan untuk tetap menjaga kerahasiaan suatu data. Dalam hal ini, kunci yang lebih panjang juga merupakan keharusan.

Saat ini, AES digunakan sebagai standard algoritma kriptografi yang terbaru. Algoritma sebelumnya dianggap tidak mampu lagi untuk menjawab tantangan perkembangan teknologi komunikasi yang sangat cepat. AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit. Dengan panjang kunci 128 bit, Misal state =19, hasil SubBytesnya = d4, ShiftRows = d4, MixColumns = 04, AddRoundKey = a4 dan proses tersebut diulang sampai 10 kali hasil ciphertextnya = 39.

Keywords : AES, enkripsi – dekripsi, kriptosistem

BAB I

PENDAHULUAN

1.1. Latar Belakang

Salah satu hal terpenting dalam komunikasi menggunakan komputer dan jaringan komputer adalah untuk menjamin keamanan pesan, data, ataupun informasi dalam proses pertukaran data, sehingga menjadi salah satu pendorong munculnya teknologi Kriptografi. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam teknik dalam upaya untuk mengamankan data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan

dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Disini enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah *system* pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat meng kodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Karena *system cipher* merupakan suatu sistem yang telah siap untuk di outomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

National Institute of Standard and Technology (NIST) untuk pertama kalinya mengumumkan suatu algoritma standar penyandian data yang telah dijadikan standart sejak tahun 1977 adalah *Data Encryption Standard* (DES). Kekuatan DES ini terletak pada panjang kuncinya yaitu 56-bit. Untuk menanggapi keinginan agar mengganti algoritma DES sebagai standart. Perkembangan kecepatan perangkat keras dan meluasnya penggunaan jaringan komputer terdistribusi mengakibatkan penggunaan DES, dalam beberapa hal, terbukti sudah tidak aman dan tidak mencukupi lagi terutama dalam hal yang pengiriman data melalui jaringan internet. Perangkat keras khusus yang bertujuan untuk menentukan kunci 56-bit DES hanya dalam waktu beberapa jam sudah dapat dibangun. Beberapa pertimbangan tersebut telah menandakan bahwa diperlukan sebuah standar algoritma baru dan kunci yang lebih panjang. Triple-DES muncul

sebagai alternative solusi untuk masalah-masalah yang membutuhkan keamanan data tingkat tinggi seperti perbankan, tetapi ia terlalu lambat pada beberapa penggunaan enkripsi.

Pada tahun 1997, the U.S. National Institue of Standards and Technology (NIST) mengumumkan bahwa sudah saatnya untuk pembuatan standar algoritma penyandian baru yang kelak diberi nama *Advanced Encryption Standard* (AES). Algoritma AES ini dibuat dengan tujuan untuk menggantikan algoritma DES & Triple-DES yang telah lama digunakan dalam menyandikan data elektronik. Setelah melalui beberapa tahap seleksi, algoritma Rijndael ditetapkan sebagai algoritma kriptografi AES pada tahun 2000.

Algoritma AES merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandi blok (*block cipher*) yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES- 128), 192-bit (AES-192), atau 256-bit (AES-256). Beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok AES di antaranya adalah *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB). Implementasi AES dengan mode operasi ECB, CBC, CFB, dan OFB tentu saja memiliki kelebihan dan kekurangan tertentu dalam aspek tingkat keamanan data.

Dalam penelitian ini, penulis tertarik untuk menggunakan algoritma tersebut untuk membantu mengamankan data. Oleh karena itu penulis memilih tugas akhir dengan judul "**Perancangan Aplikasi Kriptography – Advanced Encryption Standard**".

1.2. Perumusan Masalah

Untuk menyelesaikan semua itu, dalam tugas akhir ini akan dibahas beberapa pokok masalah, antara lain :

a. Bagaimana membuat program aplikasi kriptosistem menggunakan bahasa pemrograman Visual Basic.NET 2005?

b. Bagaimana penggunaan algoritma AES dengan bahasa pemrograman Visual Basic.NET 2005 dalam membantu keamanan aplikasi kriptosistem ?

1.3. Batasan Masalah

Pada tugas akhir kali ini akan dilakukan pembahasan mengenai hal sebagai berikut :

a. Rancangan program aplikasi ini dibuat untuk mengamankan pesan

b. Ukuran teks yang dapat dienkripsi senilai 2000 karakter, teks berupa angka dan huruf yang tersedia pada keyboard

c. Program aplikasi ini hanya dapat menyimpan file dalam format notepad (*.txt)

d. Algoritma kriptosistem ini hanya dapat mengenkripsi dan mendekripsi data yang berupa teks atau tulisan, bukan suara maupun gambar.

1.4. Tujuan

a. Membuat / merancang program aplikasi kriptosistem menggunakan bahasa pemrograman Visual Basic.NET 2005

b. Untuk mengetahui output program aplikasi kriptosistem menggunakan algoritma AES melalui bahasa pemrograman Visual Basic.NET 2005

1.5. Manfaat

a. Mempermudah user mengenkripsi dan mendekripsikan pesan

b. Melindungi kerahasiaan suatu informasi dari pihak yang tidak di harapkan

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam pembuatan skripsi ini meliputi beberapa bagian, yaitu :

a. Tinjauan pustaka

Tinjauan pustaka ini meliputi studi mengenai teori, fitur-fitur kriptografi dan algoritma AES *(Advanced Encryption Standard)*

b. Pengumpulan data

Pengumpulan data yang dilakukan meliputi pengumpulan data kriptografi dan algoritma AES *(Advanced Encryption Standard)*

c. Pengujian sistem

Pengujian sistem pada tugas akhir ini akan dilakukan dengan menjalankan aplikasi kriptosistem.

d. Pengambilan kesimpulan

Pengambilan kesimpulan berdasarkan hasil pengujian yang telah dilakukan terhadap sistem yaitu meliputi kesimpulan terhadap pengenkripsian dan pendekripsian yang akan diolah oleh aplikasi kriptosistem

e. Penulisan laporan tugas akhir

Penulisan laporan tugas akhir diambil dari hal-hal yang telah dilakukan mulai pengerjaan awal hingga selesai pengerjaan.

1.7. Sistematika Penulisan

Dalam laporan tugas akhir ini, pembahasan disajikan dalam enam bab dengan sistematika pembahasan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan pembuatan tugas akhir ini.

BAB II TINJAUAN PUSTAKA

Pada bab ini dijelaskan tentang teori-teori serta penjelasan-penjelasan yang dibutuhkan dalam pembuatan Perancangan Aplikasi Kriptography - *Advanced Encryption Standard.*

BAB III PERANCANGAN SISTEM

Bab ini dijelaskan tentang garis besar dan fokus dari rancangan aplikasi, juga berisi tentang alur proses program serta hal-hal yang diperlukan dalam implementasi. Seperti deskripsi umum sistem, spesifikasi kebutuhan sistem dan desain antarmuka.

BAB IV IMPLEMENTASI SISTEM

Pada bab ini berisikan bagaimana implementasi aplikasi yang telah dibuat berdasarkan desain yang telah dibuat dalam bab II.

BAB V UJI COBA DAN EVALUASI

Pada bab ini menjelaskan tentang pelaksanaan uji coba dan evaluasi dari pelaksanaan uji coba program yang dibuat.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran yang diperoleh dari hasil penganalisaan data dalam bab-bab sebelumnya sesuai dengan tujuan penelitian tugas akhir ini.